(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Gebrauchsmusterschrift**

(10) **DE 201 12 350 U 1**

(51) Int. Cl.[7]:
G 07 B 17/04
G 06 F 12/14

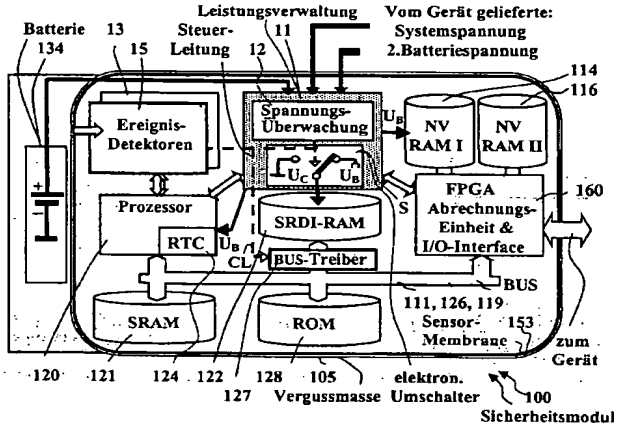
(21) Aktenzeichen: 201 12 350.9
(22) Anmeldetag: 16. 7. 2001
(47) Eintragungstag: 17. 1. 2002
(43) Bekanntmachung im Patentblatt: 21. 2. 2002

DE 201 12 350 U1

(73) Inhaber:
Francotyp-Postalia AG & Co., 16547 Birkenwerder, DE

(54) Anordnung zum Schutz eines Sicherheitsmoduls

(57) Anordnung zum Schutz eines Sicherheitsmoduls, der mindestens einen Arbeitsspeicher (121), eine Spannungsüberwachungseinheit (12), eine Ungestecktsein-Detektionseinheit (13) und einen speziellen Schaltkreis (160) aufweist, der über einen BUS mit dem Arbeitsspeicher (121) in kommunikativer Verbindung steht, wobei der speziellen Schaltkreis (160) mit einem I/O Interface zur Herstellung einer Kommunikationsverbindung mit dem Gerät ausgestattet ist, welches während des Betriebes eine Systemspannung für den Sicherheitsmodul bereitstellt, wobei letzterer von einer Langzeit-Batterie (134) außerhalb seines Betriebes gespeist wird, wobei die vorgenannten Baugruppen ohne die Langzeit-Batterie (134) in einer Vergussmasse (105) eingeschlossen sind, in welche eine Membrane (153) mit einer ersten Leiterschleife eingebettet ist, dadurch gekennzeichnet, dass eine Lösch-Hardware mit dem Arbeitsspeicher (121) verbunden ist, welche ausgestattet ist, sicherheitsrelevante Daten im Arbeitsspeicher (121) zu löschen und eine Datenabfrage über den Bus zu unterbinden, wenn ein Löschsignal anliegt, daß die Membrane (153) eine zweite Leiterschleife (152) aufweist und dass die erste und zweite Leiterschleife (151, 152) unterschiedliche Potentiale führen und auf der Membrane (153) eng benachbart angeordnet sind, dass eine Zerstörungs-Detektionseinheit (15) eingangsseitig mit der ersten und zweiten Leiterschleife (151, 152) gekoppelt und ausgangsseitig mit einem Ausgang der Spannungsüberwachungseinheit (12) über eine logische ODER-Schaltung verknüpft ist, um auf einer gemeinsamen Steuerleitung (CL) das Löschsignal für die Lösch-Hardware bereitzustellen, wenn die Zerstörungs-Detektionseinheit (15) aufgrund mindestens eines veränderten Potentials in einer der Leiterschleifen (151, 152) anspricht oder die Batteriespannung der Langzeit-Batterie (134) unter einen vorbestimmten Grenzwert absinkt.



DE 201 12 350 U1

Francotyp-Postalia AG & Co.
Triftweg 21 - 26
16547 Birkenwerder

16. Juli 2001

G3199-DE

Anordnung zum Schutz eines Sicherheitsmoduls

Beschreibung

Die Erfindung betrifft eine Anordnung zum Schutz eines Sicherheitsmoduls, gemäß der im Oberbegriff des Anspruchs 1 angegebenen Art. Ein solches Sicherheitsmodul arbeitet in einer potentiell unfreundlichen Umgebung in Geldautomaten, Fahrkartenautomaten, Registrierkassen, elektronischen Geldbörsen, Computern für den persönlichen Gebrauch (Palmtops, Notebooks, Organizers), Handys und Geräten, die mehrere dieser Funktionalitäten kombinieren. Das Sicherheitsmodul kann in Form eines postalischen Sicherheitsmoduls realisiert werden, welches insbesondere für den Einsatz in einer Frankiermaschine bzw. Postbearbeitungsmaschine oder Computer mit Postbearbeitungsfunktion (PC-Frankierer) geeignet ist.

Es sind bereits vielfältige Sicherungsmaßnahmen zum Schutz gegen Ausfälle bzw. Störungen von intelligenten elektronischen Systemen bekannt.

Es ist bereits aus EP 417 447 B1 bekannt, in elektronischen Datenverarbeitungsanlagen besondere Module einzusetzen und mit Mitteln zum Schutz vor einem Einbruch in ihre Elektronik auszustatten. Solche Module zählen zu den Sicherheitsmodulen.

Moderne Frankiermaschinen, oder andere Einrichtungen zum Frankieren von Postgut, sind mit einem Drucker zum Drucken des Postwertstempels auf das Postgut, mit einer Steuerung zum Steuern des Druckens und der peripheren Komponenten der Frankiermaschine, mit einer Abrecheneinheit zum Abrechnen von Postgebühren, die in nichtflüchtigen Speichern gehalten werden, und einer Einheit zum kryptografischen Absichern der Postgebührendaten ausgestattet. Ein Sicherheitsmodul (EP 789 333 A2) kann eine Hardware-Abrecheneinheit und/oder die Einheit zum Absichern des Druckens der Postgebührendaten aufweisen. Beispielsweise kann ersterer als Anwenderschaltkreis ASIC und letzterer als OTP-Prozessor (One Time Programmable) realisiert werden. Ein Prozessor-interner Speicher speichert auslesesicher sensible Daten (kryptografische Schlüssel), die beispielsweise zum Nachladen eines Guthabens erforderlich sind. Eine Kapselung durch ein Sicherheitsgehäuse bietet einen weiteren Schutz.

Zum Schutz eines Sicherheitsmoduls vor einem Angriff, auf die in ihm gespeicherten Daten, wurden weitere Maßnahmen vorgeschlagen, in der DE 198 16 572 A1, mit dem Titel: Anordnung für ein Sicherheitsmodul und DE 198 16 571 A1, mit dem Titel: Anordnung für den Zugriffsschutz für Sicherheitsmodule, im EP 1 035 516 A2, mit dem Titel: Anordnung für ein Sicherheitsmodul, im EP 1 035 517 A2 und EP 1 035 518 A2, beide mit dem Titel: Verfahren zum Schutz eines Sicherheitsmoduls und Anordnung zur Durchführung des Verfahrens, im EP 1 035 513 A2, mit dem Titel: Sicherheitsmodul mit Statussignalisierung, sowie im deutschen Gebrauchsmuster DE 200 20 635 U1, mit dem Titel: Anordnung zur Stromversorgung für einen Sicherheitsbereich eines Gerätes.

Zum Schutz eines Sicherheitsmoduls wurde im EP 1 035 518 A2 eine Ungestecktsein-Detektionseinheit vorgeschlagen, mit der einerseits ein Gestecktsein des Sicherheitsmoduls an ein Interface der Hauptplatine des Gerätes und andererseits ein mechanischer oder chemischer Angriff auf das Sicherheitsmodul oder dessen Beschädigung detektiert werden kann. Dabei wird ein Schaltungszustand der Detektionseinheit geändert, wobei

dessen Aufrechterhaltung durch den speziellen batteriegetriebenen Schaltungsaufbau gewährleistet ist. Eine Leitung, welche als Schleife um die übrigen Funktionseinheiten des Sicherheitsmoduls gelegt ist, gestattet dabei die Detektion einer mechanischen oder chemischen Beschädigung des Sicherheitsmoduls, wenn dabei eine Unterbrechung der Leitung eintritt. Auch beim Austausch des Sicherheitsmoduls wird diese Masseverbindung unterbrochen und die abfragbare Hardware der Ungestecktsein-Detektionseinheit registriert diesen Vorgang als Ereignis. Vom Prozessor kann der Zustand der Ungestecktsein-Detektionseinheit abgefragt werden. Die regelmäßige Auswertung eines von der Ungestecktsein-Detektionseinheit gelieferten Trennungs- bzw. Ungestecktsein-Signals ermöglicht es dem Prozessor sensitive Daten zu löschen, beispielsweise beim Entfernen des Sicherheitsmoduls aus dem Gerät. Dabei werden beispielsweise kryptographische Schlüssel gelöscht, ohne damit die Abrechnungs- und Kundendaten in den übrigen nichtflüchtigen Speichern zu verändern. Der Prozessor kann die Ungestecktsein-Detektionseinheit nach dem Stecken des Sicherheitsmodul wieder zurücksetzen. Über die Leitungsschleife wird Massepotential abgefragt, welches am Anschluß des Interfaces anliegt und nur abfragbar ist, wenn der Sicherheitsmodul ordnungsgemäß gesteckt ist. Jedoch ist eine Überbrückung der Leitungsschleife mit Massepotential nicht völlig unmöglich. Die Kenntnis der Leitungsführung ist nur durch die Einbettung in eine Vergußmasse erschwert.

Das Sicherheitsmodul ist zum Beispiel auf die Hauptplatine des Meters der Frankiermaschine JetMail® gesteckt. Das Metergehäuse ist vorzugsweise als Sicherheitsgehäuse ausgebildet ist, aber dennoch vorteilhaft so konstruiert, daß der Benutzer die Statusanzeige des Sicherheitsmoduls von außen durch eine Öffnung sehen kann. Das Anlegen der Systemspannung an den Modulprozessor des Sicherheitsmoduls ist ausreichend, die Anzeige zu aktivieren, um den Modulzustand ablesen zu können. Es kann unterschieden werden, ob das Sicherheitsmodul betriebsbereit oder defekt ist. Selbst wenn das Sicherheitsmodul funktioniert, kann signalisiert werden, wenn ein Service-Techniker zu rufen ist oder ein Restart des Systems durchgeführt wird. Ein Sicherheitsmodul kann in seinem Lebenszyklus verschiedene Zustände einnehmen, die aber nur im Betriebszustand des Meters angezeigt werden, d.h. wenn Systemspannung am Sicherheitsmodul anliegt. Anderenfalls würde die Batterie des Sicherheits-

moduls schnell erschöpft sein. Die Lebensdauer der Batterie soll dem Lebenszyklus angemessen und möglichst hoch sein. Bei ausgeschalteter Frankiermaschine, Stromunterbrechungen oder Systemspannungsausfall müssen Postregisterdaten, kryptografische Schlüssel und andere sensible Daten erhalten bleiben und auch die Echtzeituhr muß weiterlaufen. Hinzu kommen Schaltungselemente für permanente Überwachungsfunktionen, die ohne Unterbrechung weiterlaufen müssen. Hierdurch steigt der Bedarf an verfügbarem Batteriestrom mit der Folge, daß die Lebensdauer der Batterie sinkt.

Auf dem Sicherheitsmodul wurde deshalb gemäß EP 1 035 516 A2 eine auswechselbare Batterie angeordnet. Letztere kann nur dann ausgewechselt werden, wenn Systemspannung anliegt. Eine vom Prozessor abfragbare Spannungsüberwachungseinheit mit rücksetzbarer Selbsthaltung detektiert einen Spannungsausfall oder ein Absinken der Batteriespannung unter eine vorbestimmte Schwelle. Die Spannungsüberwachungseinheit hat jedoch einen nicht zu vernachlässigenden Strombedarf, was sich bei Batteriebetrieb entsprechend auswirkt.

Unter dem Titel: Verfahren zur Ermittlung eines Erfordernis zum Austausch eines Bauteils und Anordnung zur Durchführung des Verfahrens, wurde in der nicht vorveröffentlichten deutschen Patentanmeldung Nr. 100 61 665.8 bereits vorgeschlagen ein weniger stromintensives indirektes Meßverfahren zur Ermittlung der restlichen Batteriekapazität einzusetzen.

Auch kurzfristige Ausfälle der Batteriespannung von Bruchteilen einer Sekunde führen zum sofortigen Blockieren des Sicherheitsmoduls und somit Unbrauchbarwerden der Frankierfunktion der Maschine. Zum Batteriewechsel mußte bisher der postalisch gesicherte Teil der Frankiermaschine geöffnet werden. Deshalb wurde mit dem deutschen Gebrauchsmuster DE 200 20 635 U1 eine Anordnung zur Stromversorgung für einen Sicherheitsbereich eines Gerätes mittels einer externen Batterie zur Aufstockung der Batteriekapazität der internen Batterie des Sicherheitsmoduls vorgeschlagen. Die Lösung mit zwei Batterien ist natürlich aufwendiger und nur bei großen Geräten geeignet. Im deutschen Gebrauchsmuster DE 200 20 635 U1 wurde schon vorgeschlagen, eine schnelle Löschung wichtiger kryptografischer Schlüssel im statischen Arbeitsspeicher vorzunehmen, wenn die Batteriespannung unter einen Grenzwert fällt. Der Stromverbrauch ist jedoch weiterhin hoch. Die Anzahl der zu

versorgenden Baugruppen bzw. Bauelemente wurde sogar noch erhöht. Das ist für Geräte mit zweiter externer Batterie eher tragbar, zumal dann die Batteriekapazität aufgestockt ist, aus der die einzelnen Baugruppen gespeist werden. Auch der Arbeitsspeicher mit den sensitiven Daten ist nicht mehr im Prozessorschaltkreis integriert, sondern im Sicherheitsmodul als separates Bauelement angeordnet. Wenn die Beschädigung eines Bereiches des Sicherheitsmoduls sehr schnell erfolgt, welcher zufällig den Prozessor enthält, ist es möglich dass ein Teil der sensitiven Daten nicht mehr gelöscht wird. Nur wenn die sensitiven Daten alle gelöscht sind, ist deren Geheimhaltung gegeben bzw. ein Fehler aufgrund einer unsachgemäßen Handhabung des postalischen Sicherheitsmoduls ausgeschlossen.

Laut der in EP 1 035 517 A2 vorgeschlagenen Lösung arbeiten eine Spannungsüberwachungseinheit und eine Ungestecktsein-Detektionseinheit bereits zusammen, jedoch wird die Löschung von sicherheitsrelevanten Daten des einen im Mikroprozessor angeordneten Arbeitsspeichers ausgelöst, der direkt an einem prozessorinternen Bus angeschlossen ist. Damit treffen die o.g. Nachteile bezüglich Sicherheit der Löschung und Batteriestromvebrauch ebenfalls zu. Außerdem soll der Zustand des Ungestecktseins keine Löschung von Daten mehr auslösen.

Der Erfindung liegt die Aufgabe zugrunde, mit geringem Aufwand den Schutz eines Sicherheitsmoduls zu gewährleisten und dabei die Nachteile des Standes der Technik zu überwinden.

Die Aufgabe wird mit den Merkmalen der Anordnung nach Anspruch 1 gelöst.

Das Sicherheitsmodul ist austauschbar in einem Gerät angeordnet, wobei letzteres entsprechend den Einsatzfällen auswählbar ist. Das Sicherheitsmodul weist mindestens einen Arbeitsspeicher, eine Spannungsüberwachungseinheit, eine Ungestecktsein-Detektionseinheit und einen speziellen Schaltkreis auf, der über einen BUS mit dem Arbeitsspeicher in kommunikativer Verbindung steht. Der speziellen Schaltkreis enthält ein I/O Interface zur Herstellung einer Kommunikationsverbindung mit dem Gerät, welches während des Betriebes eine Systemspannung für das Sicherheitsmodul bereitstellt. Letzterer wird von einer Langzeit-Batterie außerhalb seines Betriebes gespeist. Die vorgenannten Baugruppen ohne

die Langzeit-Batterie sind in einer Vergussmasse eingeschlossen. In letztere ist ein Membrane eingebettet, mit einer ersten und zweiten Leiterschleife, die jeweils unterschiedliche Potentiale führen und auf der Membrane eng benachbart angeordnet sind. Eine mit dem Arbeitsspeicher verbundene Lösch-Hardware ist entsprechend ausgestattet, sicherheitsrelevante Daten (Secure Relevant Data Items) im SRDI-Arbeitsspeicher zu löschen und eine Datenabfrage über den Bus zu unterbinden, wenn ein Löschsignal anliegt. Eine Zerstörungs-Detektionseinheit ist eingangsseitig mit der ersten und zweiten Leiterschleife gekoppelt und ausgangsseitig mit einem Ausgang der Spannungsüberwachungseinheit über eine logische ODER-Schaltung verknüpft, um auf einer gemeinsamen Steuerleitung das Löschsignal für die Lösch-Hardware bereitzustellen, wenn die Zerstörungs-Detektionseinheit aufgrund mindestens eines veränderten Potentials in einer der Leiterschleifen anspricht oder die Batteriespannung unter einen vorbestimmten Grenzwert absinkt.

Die Erfindung geht weiterhin davon aus, dass mittels einem schnellen Mikroprozessor und weiteren teilweise bekannten Funktionseinheiten ein Sicherheitsmodul geschaffen wird, das allen Anforderungen genügt. Das Sicherheitsmodul umfaßt: einen Mikroprozessor, eine Echtzeituhr (RTC), einen Programmspeicher, einen Arbeitsspeicher, zwei nichtflüchtige Speicher für Buchungsdaten, einen SRDI-Arbeitsspeicher (Secure Relevant Data Items) mit Lösch-Hardware, eine Langzeit-Batterie (long life time), eine Leistungsverwaltungs- & Überwachungseinheit (Power Manager), Ereignisdetektoren (Event Detectors) sowie einen speziellen Schaltkreis, zum Beispiel FPGA, der mindestens dazu ausgestattet ist, mit einem I/O Interface eine Kommunikationsverbindung mit dem Gerät herzustellen.
Die Leistungsverwaltungs-& Überwachungseinheit (Power Manager) ist ausgerüstet, mindestens mit einer Spannungsüberwachungseinheit, mit Schnittstellen zur Zuführung der Systemspannung (Main Power Supply Interface) und zur Batteriespannungszuführung (Host Battery Interface). Einer der Ereignisdetektoren (Event Detectors) ist die vorgenannte Zerstörungs-Detektionseinheit, die mit der in der Vergussmasse eingebetten Membrane verbunden ist. Ein weiterer Ereignisdetektor ist eine an sich bekannte Ungestecktsein-Detektionseinheit. Die Ereignisdetektoren und die Leistungsverwaltungs-& Überwachungseinheit sind durch den Mikroprozessor abfragbar ausgebildet. Die Spannungsüberwachungseinheit oder ein Ereignisdetektor, vorzugsweise die Zerstörungs-Detektionsein-

heit, können über die gemeinsame Steuerleitung einen elektronischen Umschalter veranlassen, dass wahlweise Betriebsspannung oder Löschspannung ggf. Massepotential an den SRDI-Arbeitsspeicher angelegt wird. Eine Bus-Treibereinheit wird ebenfalls über die gemeinsame Steuerleitung angesteuert, um den BUS vom SRDI-Arbeitsspeicher zu entkoppeln, wenn Löschspannung bzw. Massepotential an den SRDI-Arbeitsspeicher angelegt wird. Bei Beschädigung des Sicherheitsmoduls und wenn die Batteriespannung die Versorgung des Sicherheitsmoduls nicht mehr sicher ermöglicht, können sensitive Daten sehr schnell und sicher gelöscht werden.

Der schnelle Prozessor ermöglicht symmetrische und/oder asymmetrische Verschlüsselungsverfahren für unterschiedlichen Einsatzfälle. Entsprechend dem jeweiligem Einsatzfall wird eine Echtzeitverarbeitung von Ereignissen sowie eine Aufzeichnung bzw. Buchung ermöglicht. Eine Batterie des Sicherheitsmoduls übernimmt die Spannungsversorgung für die Echtzeituhr und für Bauelemente zur nichtflüchtigen Speicherung der Nutzdaten, zur permanenten Überwachung aller sicherheitsrelevanten Funktionen sowie der Betriebsbereitschaft des Sicherheitsmoduls bei ausgeschalteter Systemspannung des Gerätes. Im Fehlerfall und bei Entfernung des Sicherheitsmoduls wird eine Zustandsänderung abfragbar gespeichert. Der Status des Sicherheitsmoduls ist auch nach dem Löschen vom Gerät abfragbar. Zur Signalisierung des Zustandes kann eine vorhandene Anzeigeeinheit des Gerätes oder ein Signalisierungsmittel des Sicherheitsmoduls mitbenutzt werden.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1, Blockschaltbild des Sicherheitsmoduls,

Figur 2, Detail der bekannten Spannungsüberwachungsschaltung,

Figur 3, Schaltung der Lösch-Hardware für einen SRDI-Arbeitsspeicher,

Figur 4, Darstellung einer Sensor-Membrane,

Figur 5a und 5b, Schaltungen der Ereignisdetektoren.

Die Figur 1 zeigt ein Blockschaltbild des Sicherheitsmoduls, umfassend die Baugruppen:

- einen Mikroprozessor 120 mit einer Echtzeituhr RTC,
- einen Programmspeicher ROM 128, zum Beispiel ein Flash 512K x32,
- einen Arbeitsspeicher SRAM 121, zum Beispiel ein SRAM 64K x32,
- zwei nichtflüchtige Speicher NVRAM I & NVRAM II mit je 4 Kbyte,
- einen Arbeitsspeicher SRDI-RAM 122 (Secure Relevant Data Items) mit Lösch-Hardware und BUS-Treibereinheit 127,
- eine Langzeit-Batterie 134, zum Beispiel eine Lithium-Batterie,
- eine Leistungsverwaltungs-& Überwachungseinheit (Power Manager) 11 mit Spannungsüberwachungseinheit 12, mit Schnittstellen zur Zuführung der Systemspannung (Main Power Supply Interface) und zur Batteriespannungszuführung (Host Battery Interface),
- Ereignisdetektoren(Event Detectors), einschließlich einer Zerstörungs-Detektionseinheit 15, die mit einer in einer Vergussmasse 105 eingebetten Membrane 153 verbunden ist, und einer Ungestecktsein-Detektionseinheit 13,
- einen speziellen Schaltkreis, zum Beispiel FPGA, 160 mit einem I/O Interface zur Herstellung einer Kommunikationsverbindung mit dem Gerät.

Das Gerät, an welchem das Sicherheitsmodul angeschlossen ist, liefert eine Systemspannung und optional eine zweite Batteriespannung. Das Sicherheitsmodul wird bei eingeschaltetem Gerät mit Systemspannung betrieben. Die Leistungsverwaltungseinheit (Power Manager) 11 hat eine Vielzahl an Funktionseinheiten, die die Betriebsfähigkeit bei geringem Leistungsverbrauch des Sicherheitsmoduls auch bei abgeschaltetem Gerät sichern. Die Leistungsverwaltungseinheit 11 weist einen Gleichstrom/Gleichstrom-Wandler (nicht gezeigt) und einen Spannungsregler (nicht gezeigt) für die entsprechenden Betriebsspannungen (3V, 5V und 8V), eine Temperatur- und Spannungsüberwachungsschaltung (nicht gezeigt) auf. Die letzteren beiden können ein Reset-Signal erzeugen. Die gelieferte Systemspannung wird auf Über- bzw. Unterschreitung von Grenzwerten überwacht. Innerhalb letzterer sorgt ein Gleichstrom/Gleichstrom-Wandler

für eine vorbestimmte Betriebsspannung U_B. Eine Spannungsgenerierung sorgt für die Erzeugung aller notwendigen Spannungen, die die Funktionseinheiten des Sicherheitsmoduls benötigen. Bei ausgeschalteten Gerät werden neben den Überwachungsschaltungen und der Zerstörungs-Detektionseinheit nur die Echtzeituhr RTC und die Arbeitsspeicher mit Batteriespannung versorgt. Eine ununterbrochene Versorgung der batteriebetriebenen Einheiten ist auch in DE 200 20 635 U1 mitgeteilt worden. Zu letzteren gehört mindestens einer der Post-Speicher, einige der Detektoren und der SRDI-Arbeitsspeicher 122. An das Sicherheitsmodul können zwei unabhängige Batterien angeschlossen werden. Die erste Batteriespannung stammt aus der internen Batterie 134, welch optional durch eine zweite separate Batterie gestützt werden kann.

Alternativ zur internen Echtzeituhr kann eine separate Echtzeituhr RTC 124 angeschlossen werden. Der Mikroprozessor 120 ist beispielsweise vom Typ ARM7 und die separate Echtzeituhr vom Typ EPSON RTC-4543. Der Mikroprozessor 120 ist über einen BUS mit dem Programmspeicher ROM 128, dem Arbeitsspeicher SRAM 121, dem Arbeitsspeicher SRDI-RAM 122 und dem speziellen Schaltkreis FPGA 160 verbunden. Der Bus ist mit breiten weißen Pfeilen dargestellt. Der spezielle Schaltkreis FPGA 160 ist ein anwerderspezifisch programmiertes FPGA (one time programmable). Der FPGA enthält eine Hardware-Abrechnungseinheit (nicht gezeigt), eine Ansteuerschaltung für zwei weitere Speicher NVRAM I und II sowie eine Ein/Ausgabe-Schnittstelle (digitale Interface des Sicherheitsmoduls nicht gezeigt) zum Gerät (nicht gezeigt). Der spezielle Schaltkreis FPGA 160 ist mit zwei nichtflüchtigen Speichern 114 (NVRAM I) & 116 (NVRAM II) verbunden, die unter anderem die postalisch relevanten Daten enthalten. Die beiden nichtflüchtigen Speicher NVRAM I und II sind physikalisch getrennt und in verschiedenen Technologien ausgeführt. Sie sind vom Prozessor schreibend und lesend ansprechbar, vom FPGA modifizierbar und von außerhalb des Sicherheitsmodules lesbar. Einer der nichtflüchtigen Speicher ist in einer gemischten EEPROM-SRAM-Technologie ausgeführt, der andere ist ein SRAM mit herkömmlicher Technologie.

Die Zuführung der Systemspannung (Main Power Supply Interface) und der Batteriespannungen zur Schnittstelle ist mit breiten schwarzen Pfeilen gekennzeichnet worden. Dünne schwarze Pfeile gekennzeichnen die Versorgung von Baugruppen mit einer entsprechenden Betriebsspannung aus der Leistungsverwaltungs-und Überwachungseinheit 11 bzw. aus der Überwachungseinheit 12. Dünne weiße Pfeile kennzeichnen Abfrage- und Steuerleitungen.

Zur Lösch-Hardware gehören teilweise Mittel der Leistungsverwaltungs-& Überwachungseinheit, eine Steuerleitung CL und eine Bus-Treibereinheit 127. Die Steuerleitungen von der Zerstörungs-Detektionseinheit 15 und der Spannungsüberwachungseinheit 12 sind zu einer gemeinsamen Steuerleitung CL verschaltet, welche gestrichelt dargestellt ist. Die Einheiten 12 oder 15 steuern über die gemeinsame Steuerleitung CL einen elektronischen Umschalter S an, welcher wahlweise Betriebsspannung U_B oder Löschspannung U_C bzw. Massepotential U_M an den VCC-Pin des SRDI-Arbeitsspeicher 122 anlegt. Dieser SRDI-RAM-Speicher ist nicht direkt an dem Prozessorbus angeschlossen. Alle digitalen Signale werden über Treiberschaltkreise der Bus-Treibereinheit 127 geführt, die über Ausgänge verfügen, die hochohmig geschaltet werden können. Damit kann der BUS vom SRDI-Arbeitsspeicher 122 entkoppelt werden. Die Bus-Treibereinheit 127 wird ebenfalls von der gemeinsamen Steuerleitung CL angesteuert.

Folgende Detektor- und Überwachungsseinheiten überwachen den sachgemäßen Betrieb des Sicherheitsmoduls:

- Spannungsüberwachungseinheit 12, die zur Batteriespannungsüberwachung mit Selbsthaltung ausgebildet ist,
- Zerstörungsdetektionseinheit 15 zur Detektion gegen mechanische Zerstörung des Sicherheitsmoduls mit Selbsthaltung,
- Ungestecktsein-Detektioneinheit 13 (Host-System-Loop) mit Selbsthaltung.
- Temperatursensor und weitere
- Spannungsüberwachungseinheiten zur Überwachung aller Spannungen im System, insbesondere der Systemspannung.

Die beiden ersten führen bei Ansprechen (oder-Verknüpfung) zum Löschen der Daten im SRDI-Speicher.

Der dritte Detektor kann nur einen Zustandswechsel hervorrufen und vom Prozessor während des Betriebes bzw. beim Systemstart vom Programm des Sicherheitsmoduls abgefragt werden.

Der Temperatursensor überwacht die Betriebstemperatur des Moduls und löst einen Reset aus, wenn die Temperatur unter oder über einen vorherbestimmten Wert sinkt bzw. steigt. Auch damit wird ein unsachgemäßer Gebrauch verhindert und die Nutzerdaten gesichert. Ein Reset wird ebenfalls ausgelöst, wenn die Eingangsspannung des Moduls zu klein oder zu groß wird oder wenn die interne Betriebsspannung unter einen bestimmten Pegel sinkt. Der Zustand aller anderen Spannungen können von der Systemsoftware abgefragt werden. Das Sicherheitsmodul enthält – nicht gezeigte - LED zur Statusausgabe und wird mit einer harten, undurchsichtigen Vergußmasse 105 vergossen, in welche eine Sensor-Membrane 153 eingebettet ist. Einer der Ereignisdetektoren, die Zerstörungs-Detektioneinheit 15, ist mit Leiterschleifen der Sensor-Membrane 153 verbunden.

Die Figur 2 zeigt ein Detail der aus dem EP 1 035 516 A2 bekannten Spannungsüberwachungsschaltung 12', die über eine Leitung 138' mit einem statischen Arbeitsspeicher SRAM 122' verbunden ist. Die Spannungsüberwachungseinheit 12' enthält einen elektronischen FET-Schalter 1252', der bei Bedarf Massepotential an den SRDI-Arbeitsspeicher 122' angelegt. Sinkt die Batteriespannung unter einen Grenzwert, dann steuert einer Operationsverstärker 1250' über eine Steuerleitung 1251' den elektronischen FET-Schalter 1252' an und mit der Leitung 138' wird der Speisepunkt (VCC-PIN) für das SRAM 122' vom elektronischen FET-Schalter 1252' der Überwachungseinheit 12' mit Masse verbunden. Die Source-Schaltung weist einen Widerstand 1254' zwischen Drain des MOSFET 1252 und einer die Betriebsspannung U_B führenden Leitung auf. Das verursacht auch weiterhin einen nicht zu vernachlässigenden Stromverbrauch, solange sich die Schaltung noch im

Schaltungs-Zustand der Selbsthaltung befindet. Der Schaltungs-Zustand kann via Entkopplungsdiode 1262' und über die Leitung 164' vom Prozessor abgefragt werden.

In der Figur 3 ist eine Schaltung der Lösch-Hardware für einen SRDI-Arbeitsspeicher 122 dargestellt. Für den SRDI-Arbeitsspeicher 122 wird vorzugsweise ein Typ BS62LV256TI eingesetzt. Es genügt bei diesem Typ, wenn zum Löschen Massepotential U_M an den VCC-Pin des SRDI-Arbeitsspeichers 122 angelegt wird. Weiterhin ist der VCC-Pin des SRDI-Arbeitsspeichers 122 ist an den elektronischen Umschalter S angeschlossen. Letzterer ist beispielsweise in die Spannungsüberwachungseinheit 12 integriert und weist einen Feld-Effekt-Transistor-Umschalter 1252, 1253 auf. Der FET-Umschalter 1252, 1253 legt wahlweise Betriebsspannung U_B oder Massepotential U_M an den VCC-Pin des SRDI-Arbeitsspeichers 122 an. Bei einem ausgeschaltetem Gerät wird automatisch von Systemspannung auf die Batteriespannung umgeschaltet. Die Betriebsspannung U_B entspricht dann der Batteriespannung. Liegt die Batteriespannung über einem Grenzwert, dann wird vom Transistor 1253 (MOSFET, Verarmungstyp, p-Kanal) Betriebsspannung auf die Leitung 138 durchgeschaltet und der Speisepunkt am VCC-Pin des SRDI-Arbeitsspeicher 122 ist mit Betriebsspannung verbunden. Der SRDI-Arbeitsspeicher 122 dient dann als batteriegestützter nichtflüchtiger Speicher für sicherheitsrelevante Daten.

Sinkt die Batteriespannung unter einen Grenzwert, dann wird der Speisepunkt am VCC-Pin des SRAMs 122 via Leitung 138 von einem Transistor 1252 (MOSFET, Verarmungstyp, n-Kanal) der Überwachungseinheit 12 mit Masse verbunden. Durch die zusatzlich vorgenommene Abschaltung des Transistors 1253 wird der Strombedarf aus der Batterie 134 (Fig.1) erheblich reduziert.

Die BUS-Treibereinheit 127 der Lösch-Hardware stellt den Weiterbetrieb der übrigen Baugruppen sicher, die ebenfalls an den Bus gekoppelt sind. Der Bus besteht aus einem Adressen-BUS 111, einem Daten-BUS 126 und einem Steuer-BUS 119. Die Ausgangsleitungen 158, 159 der

Zerstörungs-Detektionseinheit 15 können via wired-OR-Verbindung verbunden werden. Ein Negator N negiert das Signal. Alternativ liefert die Zerstörungs-Detektionseinheit 15 ein geeignetes Signal auf mindestens einer Ausgangsleitung, welche mit der Steuerleitung 1251 der Spannungsüberwachungseinheit 12 mittels ODER-Glied zur gemeinsamen Steuerleitung CL verschaltet sind. Das ODER-Glied kann auch als wired-OR-Verbindung 1255 in der Spannungsüberwachungseinheit 12 ausgebildet sein. Wenn also die Einheiten 12 oder 15 einen unsachgemäßen Gebrauch des Sicherheitsmoduls detektieren, so werden gleichzeitig die Treiberschaltkreise hochohmig geschaltet und der Transistor-Umschalter wird so angesteuert, daß der VCC-Pin des SRDI-Speichers auf Massepotential U_M liegt. Der Vorteil dieser Anordnung ist, das der SRDI-Speicher vollständig spannungsfrei ist und die Daten schnell zerstört werden, denn CMOS-Schaltungen sind ja bekannt dafür, daß sie sich auch über ihre digitalen Eingänge sebst versorgen können. Zweitens wird der SRDI-Speicher über die Treiber so vom Prozessorbus getrennt, daß letztere in seiner Tätigkeit nicht beeinflusst wird und weiter arbeiten kann. Die Detektion und die Reaktion darauf funktioniert sowohl beim Betrieb mit Systemspannung als auch mit Batteriespannung.

Mindestens eine Leiterschleife umhüllt die Baugruppen bzw. Funktionseinheiten des Sicherheitsmoduls, welche zusätzlich mit einer Vergußmasse vergossen sind, was prinzipiell im EP 1 035 518 A2 bereits dargestellt ist. Jedoch bei Bekanntheit der genauen Leitungsführung wird eine Überbrückung einer Leiterschleife möglich. Die Kenntnis der Leitungsführung ist dort nur durch die Vergußmasse erschwert. In Ergänzung dazu ist vorgesehen, dass nicht mehr nur Masseschluß, sondern zusätzlich eine Veränderung mindestens eines weiteren Potentials ausgewertet wird. An die Zerstörungs-Detektionseinheit 15 sind vorzugsweise zwei Leitungsschleifen 151 und 152 angeschlossen, welche nebeneinander isoliert auf einer Sensor-Membran 153 liegen. Die Leitungsschleifen 151, 152 führen unterschiedliche Spannungspotentiale. Bei einer geeigneten Leitungsführung sind die unterschiedlichen Spannungspotentiale eng benachbart. Damit wird eine absichtliche Überbrückung einer Leiterschleife wenigstens erschwert. Jede grobe Zerstörung der Vergußmasse führt zu einer Zer-

störung der Leitungsschleifen 151 und 152 oder wenigstens zu einer detektierbaren Potentialveränderung. Eine Überbrückung der Leitungsschleifen 151, 152 wird durch eine spezielle Leitungsführung noch weiter erschwert.

Die Figur 4 zeigt eine Darstellung einer Sensor-Membrane am Beispiel einer einfachen Ausführungsform. Natürlich können andere kompliziertere Ausführungsformen gewählt werden. Wichtig ist nur, dass auf engem Raum eine solche Leitungsführung gewählt wird, dass unterschiedliche Potentiale eng benachbart sind, so dass eine Überbrückung von Leitungsabschnitten unmöglich gemacht wird, ohne die Potentiale zu verändern.

Die Figuren 5a und 5b zeigen Schaltungen für eine Zerstörungs-Detektion. Die in der Figur 5a gezeigte Detektionsschaltung 15a weist einen Spannungsteiler zwischen einer Batteriespannung führenden Leitung 156 und Massepotential auf, wobei der Widerstand der Leitungsschleife 151 zwischen die Leitung 156 und einem Abzweig 1546 des Spannungsteilers geschaltet ist. Zwischen den Abzweig 1546 des Spannungsteilers und Massepotential ist eine Parallelschaltung von Widerstand 1544 und Kondensator 1572 geschaltet. Die Detektionsschaltung 15a dient der Leitungsschleifen-Überwachung und reagiert auf eine Absenkung des Spannungspotentials am Abzweig 1546 unter einen ersten Referenzspannungswert. Eine solche Absenkung ist durch Verringerung der Isolation gegenüber dem Massepotential in der Leitungsschleife 151 nahe dem Abzweig 1546 oder durch schleichende Hochohmigkeit, infolge einer fortschreitenden Veringerung des Leitungsquerschnitts bis zur Unterbrechung der Leitungsschleife 151 verursacht.
Die Schaltung ist im Prinzip ähnlich der Schaltung der bereits aus dem EP 1 035 516 A2 bekannten Spannungsüberwachungseinheit 12´ aufgebaut, welche ebenda ausführlicher beschrieben ist.
Die Batteriespannung auf der Leitung 156 wird am Abzweig 1546 des Spannungsteilers entsprechend verringert abgegeben und von einem Komparator 1550 mit der Referenzspannung der Referenzspannungsquelle 1548 verglichen. Ist die zu vergleichende Spannung auf dem Ab-

zweig 1546 kleiner als die Referenzspannung, so erhält ein Feld-Effekt-Transistor 1552 an seinem Steuereingang H-Pegel und wird durchgeschaltet. Dadurch wird die Ausgangsleitung 158 mit Massepotential verbunden und der SRDI-RAM 122 wird nicht mehr mit der Batteriespannung versorgt. Das führt zur Löschung der Daten im SRDI-RAM 122.

Da die Leitung 158 jetzt Massepotential führt, wird gleichzeitig über die Diode 1556 und den Widerstand 1558 die zu vergleichende Spannung am Abgriff 1546 auf einen Wert nahe 0 V gezogen. Dadurch wechselt die Überwachungsschaltung 15a in einen Selbsthaltezustand, in dem sie auch bei Erhöhung der Spannung am Abgriff 1546 verharrt und die Leitung 158 auf Massepotential läßt. Durch diesen Zustand der Detektionsschaltung 15a wird über eine Entkopplungsdiode 1562 ein L-Signal auf die Leitung 157 gelegt, welche vom Prozessor 120 abgefragt werden kann. Die Entkopplungsdiode 1562 dient der Verringerung des Stromverbrauchs im Batteriebetrieb. Der Prozessor 120 kann die Detektionsschaltung 15a zurücksetzen. Dazu wird über die Leitung 155 ein H-Rücksetzsignal auf einen Feld-Effekt-Transistor 1560 gegeben, welcher durchgeschaltet wird, Somit wird die Spannung am Abzweig 1546 über die Referenzspannung angehoben, der Komparator 1550 schaltet zurück und der Transistor 1552 wird gesperrt. Als Komparator 1550 eignet sich der Typ ICL7665SAIBA.

Die in der Figur 5b gezeigte Detektionsschaltung 15b weist einen Spannungsteiler zwischen einer Batteriespannung führenden Leitung 156 und Massepotential auf, wobei eine Parallelschaltung von Kondensator 1573 und dem Widerstand der Leitungsschleife 152 zwischen Massepotential und einem Abzweig 1547 des Spannungsteilers geschaltet ist. Zwischen den Abzweig 1547 des Spannungsteilers und der Leitung 156 ist ein Widerstand 1545 geschaltet. Die Detektionsschaltung 15b dient der Leitungsschleifen-Überwachung und reagiert auf eine Erhöhung des Spannungspotentials am Abzweig 1547 über einen zweiten Referenzspannungswert. Eine solche Erhöhung ist durch Verringerung der Isolation gegenüber dem Spannungpotential in der Leitungsschleife 151 nahe dem Abzweig 1547 oder durch schleichende Hochohmigkeit, infolge einer fortschreitenden Veringerung des Leitungsquerschnitts bis zur Unter-

brechung der Leitungsschleife 152 verursacht. Am Abzweig 1547 ist der nichtinvertierende Eingang eines Komparators 1551 angeschlossen. Der invertierende Eingang des Komparators 1551 ist mit einer Referenzspannungsquelle 1549 verbunden. Der Ausgang des Komparators 1551 ist über einen Negator 1553, 1555 mit der Leitung 159 verbunden. Der zwischen dem Abgriff 1547 und Masse geschaltete Kondensator 1573 verhindert Schwingungen. Die Spannung am Abgriff 1547 des Spannungsteilers wird im Komparator 1551 mit der Referenzspannung der Referenzspannungsquelle 1549 verglichen. Ist die zu vergleichende Spannung am Abgriff 1547 kleiner als die Referenzspannung der Quelle 1549, so bleibt der Komparatorausgang auf L-Pegel geschaltet und der Feld-Effekt-Transistor 1553 des Negators ist gesperrt. Dadurch erhält die Ausgangsleitung 159 nun Betriebsspannungspotential und das Statussignal führt logisch '1'. Wird jedoch das Spannungspotential am Abzweig 1547 über die Referenzspannung der Referenzspannungsquelle 1549 erhöht, dann schaltet der Komparator 1551 um. Der Komparatorausgang wird auf H-Pegel geschaltet und folglich ist der Feld-Effekt-Transistor 1553 durchgeschaltet. Dadurch wird die Ausgangsleitung 159 mit Massepotential verbunden und das Statussignal führt logisch '0.

Es ist vorgesehen, daß die Mittel der Detektionsschaltung 15a von der Detektionsschaltung 15b mit benutzt werden, so dass eine separate Abfrageleitung, ein separates Schaltungsmittel zur Selbsthaltung und ein Schaltmittel für eine Rücksetzung der Selbsthaltung in der Detektionsschaltung 15b entfällt. Dazu ist die Ausgangsleitung 159 der Detektionsschaltung 15b mit der Ausgangsleitung 158 der Detektionsschaltung 15a verbunden.

Die Überwachungsschaltung 15b ist im Prinzip ähnlich der Schaltung der bereits aus dem EP 1 035 517 A2 bekannten Ungestecktsein-Detektionseinheit 13 aufgebaut, welche ebenda ausführlicher beschrieben ist. Die Überwachungsschaltung 15b benötigt im Unterschied jedoch keine separaten Schaltungsmittel zur Selbsthaltung und deren Rücksetzung.

Alternativ ist eine Schaltung einsetzbar, welche ein negiertes Ausgangssignal liefert. Vorzugsweise kann dann ein Verbinden der Ausgangsleitun-

gen 158 und 159 mittels der in der Überwachungsschaltung 12 vorgesehenen wired-OR-Verknüpfung vorgenommen werden.
Als Ereignisdetektoren (Event Detectors), werden neben der Zerstörungs-Detektionseinheit 15 auch eine Ungestecktsein-Detektionseinheit 13 eingesetzt, die in dem EP 1 035 517 A2 ausführlicher beschrieben ist. Im Unterschied dazu erfolgt jedoch keine logische Verknüpfung mit Signalen einer der anderen Baugruppen bzw. Funktionseinheiten.

Das Sicherheitsmodul, welches zum Einsatz in postalischen Geräten, insbesondere zum Einsatz in einer Frankiermaschine, bestimmt ist, wird als postalisches Sicherheitsmodul (Postal Security Device) oder als sicheres Abrechnungsgerät (Security Accounting Device) bezeichnet. Jedoch kann das Sicherheitsmodul auch eine andere Bauform aufweisen, die es ermöglicht, daß es in unterschiedlichen Geräten arbeiten kann. Somit wird es ermöglicht, dass es beispielsweise auf die Hauptplatine eines Personalcomputers gesteckt werden kann, der als PC-Frankierer einen handelsüblichen Drucker ansteuert.

Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die - vom gleichen Grundgedanken der Erfindung ausgehend - von den anliegenden Schutzansprüchen umfaßt werden.

***

Schutzansprüche

1. Anordnung zum Schutz eines Sicherheitsmoduls, der mindestens einen Arbeitsspeicher (121), eine Spannungsüberwachungseinheit (12), eine Ungestecktsein-Detektionseinheit (13) und einen speziellen Schaltkreis (160) aufweist, der über einen BUS mit dem Arbeitsspeicher (121) in kommunikativer Verbindung steht, wobei der speziellen Schaltkreis (160) mit einem I/O Interface zur Herstellung einer Kommunikationsverbindung mit dem Gerät ausgestattet ist, welches während des Betriebes eine Systemspannung für den Sicherheitsmodul bereitstellt, wobei letzterer von einer Langzeit-Batterie (134) außerhalb seines Betriebes gespeist wird, wobei die vorgenannten Baugruppen ohne die Langzeit-Batterie (134) in einer Vergussmasse (105) eingeschlossen sind, in welche eine Membrane (153) mit einer ersten Leiterschleife eingebettet ist, dadurch gekennzeichnet, dass eine Lösch-Hardware mit dem Arbeitsspeicher (121) verbunden ist, welche ausgestattet ist, sicherheitsrelevante Daten im Arbeitsspeicher (121) zu löschen und eine Datenabfrage über den Bus zu unterbinden, wenn ein Löschsignal anliegt, daß die Membrane (153) eine zweite Leiterschleife (152) aufweist und dass die erste und zweite Leiterschleife (151, 152) unterschiedliche Potentiale führen und auf der Membrane (153) eng benachbart angeordnet sind, dass eine Zerstörungs-Detektionseinheit (15) eingangsseitig mit der ersten und zweiten Leiterschleife (151, 152) gekoppelt und ausgangsseitig mit einem Ausgang der Spannungsüberwachungseinheit (12) über eine logische ODER-Schaltung verknüpft ist, um auf einer gemeinsamen Steuerleitung (CL) das Löschsignal für die Lösch-Hardware bereitzustellen, wenn die Zerstörungs-Detektionseinheit (15) aufgrund mindestens eines veränderten Potentials in einer der Leiterschleifen (151, 152) anspricht oder die Batteriespannung der Langzeit-Batterie (134) unter einen vorbestimmten Grenzwert absinkt.

2. Anordnung, nach Anspruch 1, dadurch g e k e n n z e i c h n e t, dass die Lösch-Hardware einen elektronischen Umschalter (S) und eine Bus-Treibereinheit (127) aufweist, dass die Bus-Treibereinheit zwischen den Daten., Adress- und Steuerungs-BUS-Leitungen (126, 111, 119) und den Daten-, Adress- und Steuerungs-Pins des Arbeitsspeicher (121) geschaltet ist und über die gemeinsame Steuerleitung (CL) ansteuerbar ist, um den BUS vom Arbeitsspeicher (121) zu entkoppeln, wenn die Spannungsüberwachungseinheit (12) oder die Zerstörungs-Detektionseinheit (13) über die gemeinsame Steuerleitung (CL) den elektronischen Umschalter (S) veranlassen, Löschspannung statt der Betriebsspannung an den VCC-Pin des Arbeitsspeichers (120) anzulegen.

3. Anordnung, nach Anspruch 2, dadurch g e k e n n z e i c h n e t, dass Massepotential anstatt der Löschspannung an den Arbeitsspeicher (122) angelegt wird.

4. Anordnung, nach Anspruch 2, dadurch g e k e n n z e i c h n e t, dass digitale Signale über Treiberschaltkreise der Bus-Treibereinheit (127) geführt werden, die über Ausgänge verfügen, die zur Entkopplung von BUS und Arbeitsspeicher (122) hochohmig geschaltet werden können.

5. Anordnung, nach Anspruch 2, dadurch g e k e n n z e i c h n e t, dass Anzahl an Leiterschleifen (151, 152) zum Schutz des Sicherheitsmoduls angeordnet sind, dass die Zerstörungsdetektionseinheit (15) mit einer entsprechenden Anzahl an Detektionsschaltungen (15a, 15b) für jede der unterschiedliche Potentiale führenden Leiterschleifen (151, 152) ausgestattet ist, wobei nur eine der Detektionsschaltungen (15a, 15b) mit einer für alle wirksamen Selbsthalteschaltung ausgestattet ist und wobei die Ausgangsleitungen (158, 159) aller Detektionsschaltungen (15a, 15b) via wired-OR-Verbindung verbunden sind.

6. Anordnung, nach Anspruch 5, dadurch g e k e n n z e i c h n e t, dass der Schaltzustand aller Detektionsschaltungen (15a, 15b) vom Mikroprozessor (120) abfragbar und dass die Selbsthalteschaltung rücksetzbar ausgebildet ist.

7. Anordnung, nach Anspruch 2, dadurch g e k e n n z e i c h n e t, dass der elektronische Umschalter (S) Bestandteil der Spannungsüberwachungseinheit (12) ist, deren von einer Selbsthalteschaltung gehaltener Schaltzustand vom Mikroprozessor (120) abfragbar und deren Selbsthalteschaltung rücksetzbar ausgebildet ist.

8. Anordnung, nach den Ansprüchen 2 und 7, dadurch g e k e n n z e i c h n e t, dass an Betriebsspannungspotential und Massepotental geschaltete Feld-Effekt-Transistoren (1252, 1253) den elektronischen Umschalter (S) bilden.

9. Anordnung, nach Anspruch 1, dadurch g e k e n n z e i c h n e t, dass die logische ODER-Schaltung als wired-OR-Verbindung in der Spannungsüberwachungseinheit (12) ausgebildet ist und die gemeinsame Steuerleitung (CL) bildet.

*****

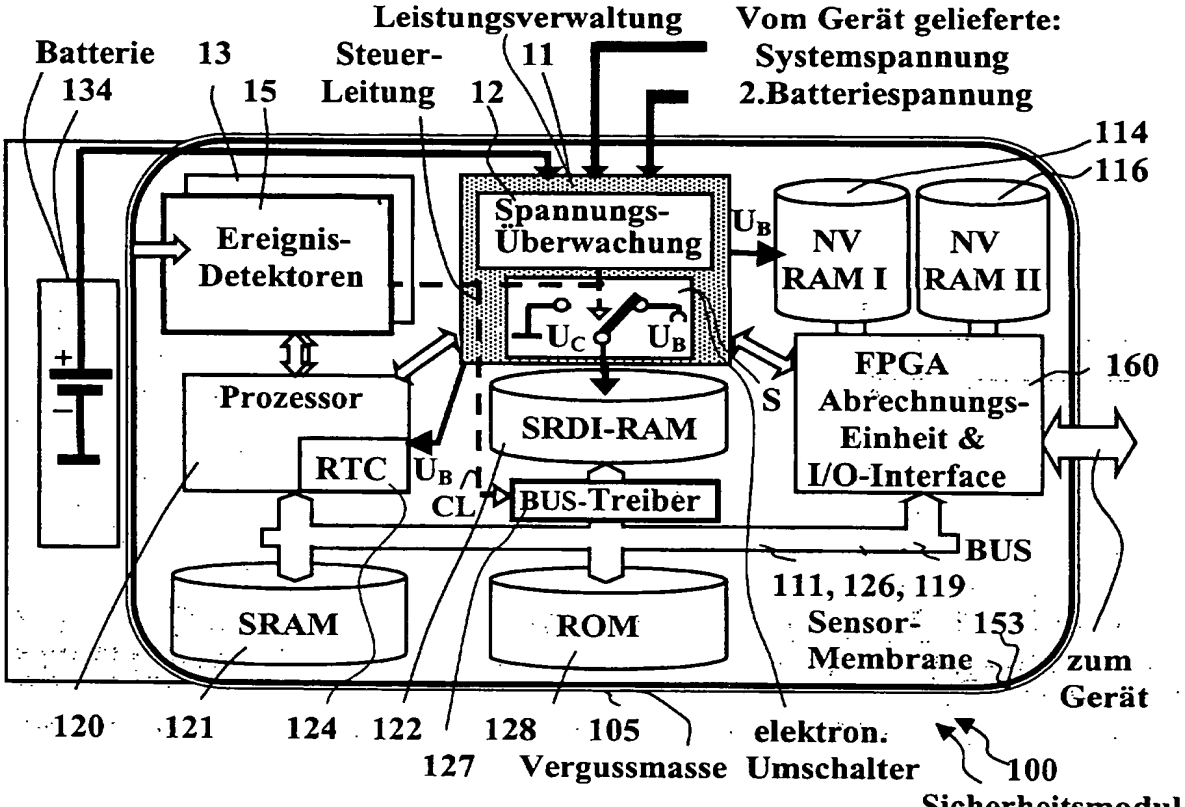

Batterie
134
13
15
Steuer-
Leitung
12
Leistungsverwaltung
11
Vom Gerät gelieferte:
Systemspannung
2.Batteriespannung
114
116
Ereignis-
Detektoren
Spannungs-
Überwachung
U_B
NV
RAM I
NV
RAM II
U_C
U_B
FPGA
Abrechnungs-
Einheit &
I/O-Interface
160
Prozessor
S
SRDI-RAM
RTC
U_B
CL
BUS-Treiber
BUS
111, 126, 119
Sensor-
Membrane
153
zum
Gerät
SRAM
ROM
120
121
124
122
128
105
127
Vergussmasse
elektron.
Umschalter
100
Sicherheitsmodul

Fig. 1

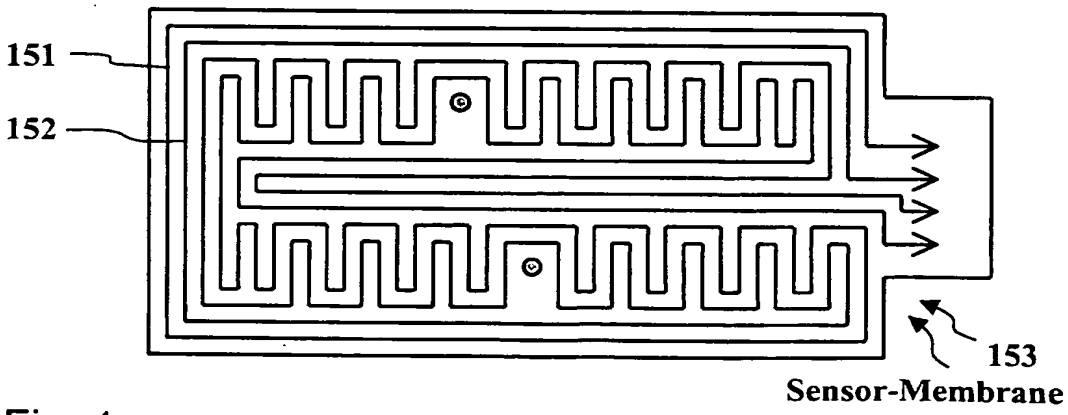

151
152
153
Sensor-Membrane

Fig. 4

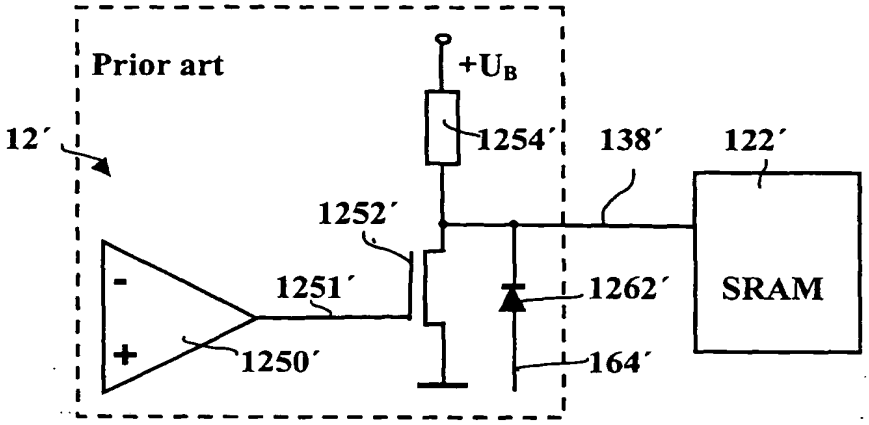

Prior art
+UB
12´
1254´
138´
122´
1252´
1251´
1262´
SRAM
1250´
164´

Fig. 2

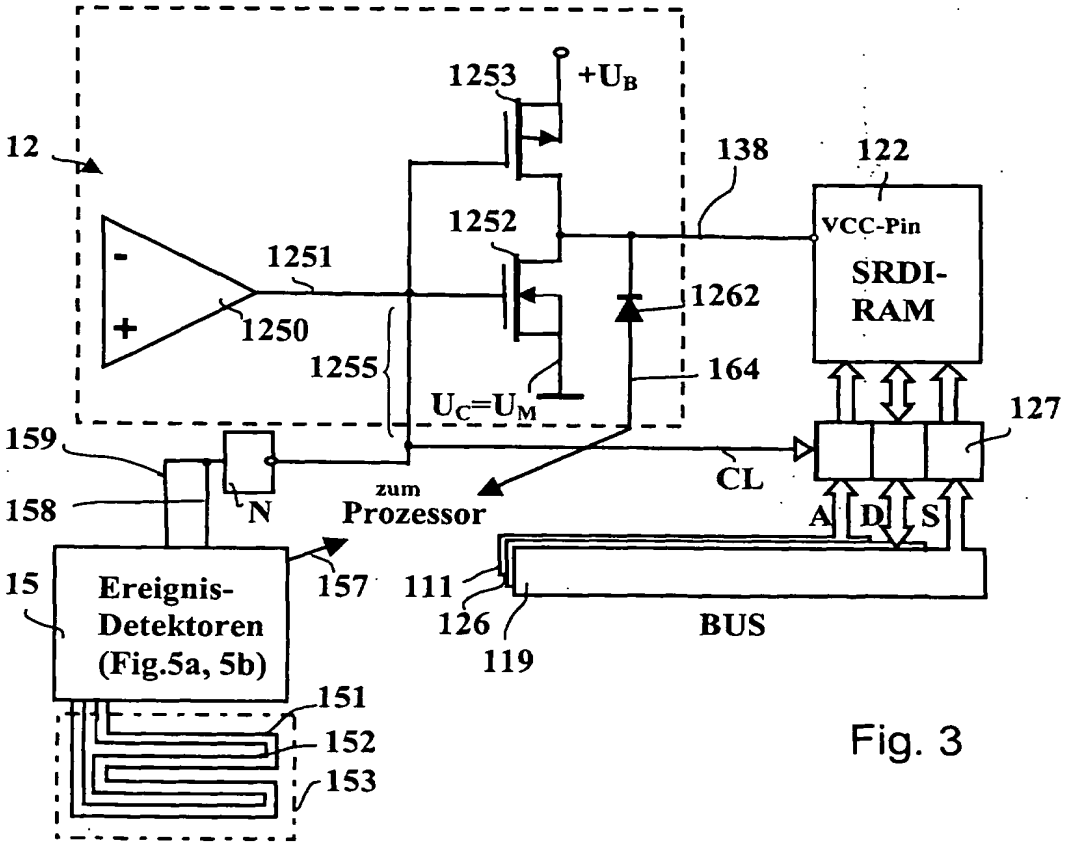

1253
+UB
12
138
122
1252
VCC-Pin
SRDI-
RAM
1251
1262
1250
1255
164
UC=UM
127
159
CL
zum
Prozessor
158
N
A
D
S
15
Ereignis-
Detektoren
(Fig.5a, 5b)
157
111
126
119
BUS
151
152
153

Fig. 3

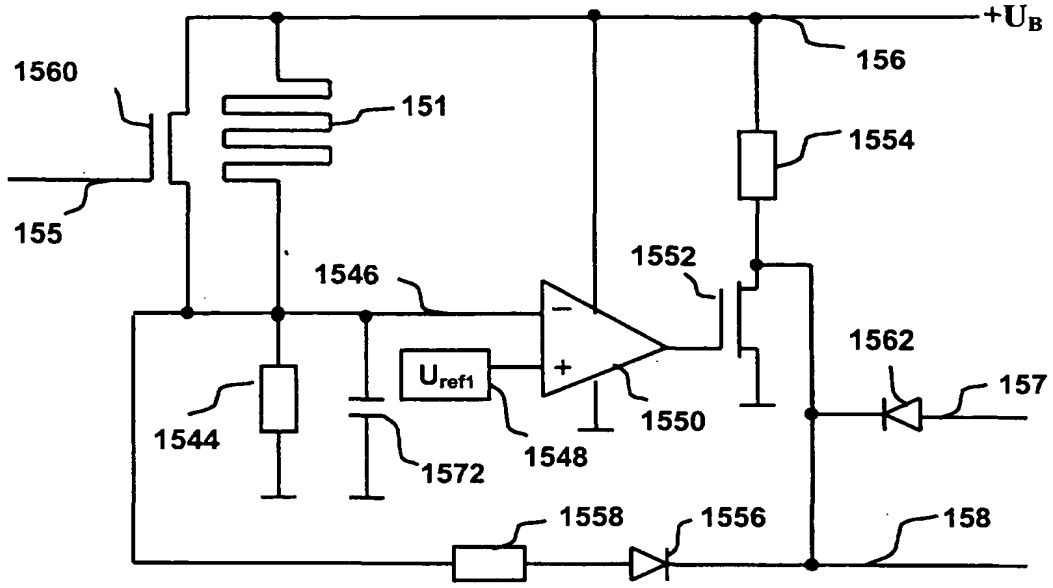

+U_B
156
1560
151
1554
155
1552
1546
1562
157
U_ref1
1544
1550
1548
1572
1558
1556
158

Fig. 5a

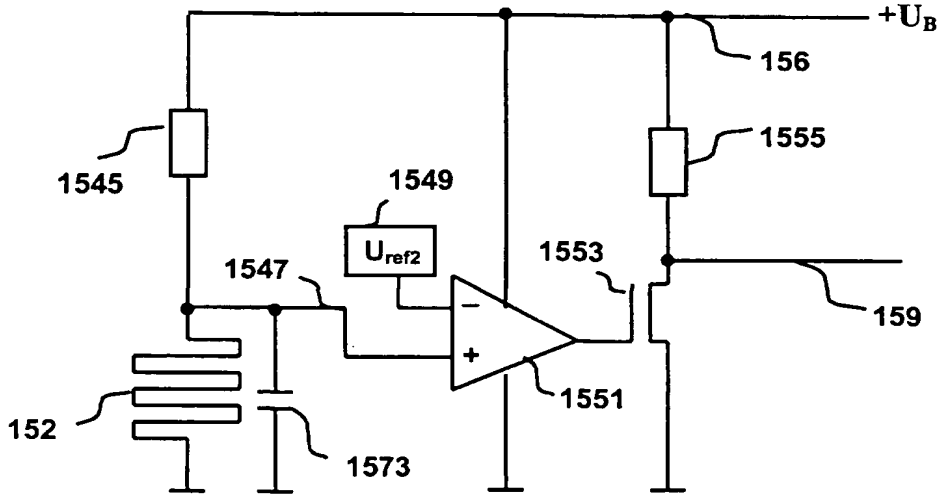

+U_B
156
1555
1545
1549
U_ref2
1553
1547
159
1551
152
1573

Fig. 5b